

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Richard Bussiere et al.
Serial No.: 10/713,560
Filed: November 14, 2003
For: DISTRIBUTED INTRUSION RESPONSE SYSTEM
Assignee: Enterasys Networks, Inc.
Examiner: Christopher Brown
Art Unit: 2134 Confirmation No. 8242

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SECOND DECLARATION OF RICHARD GRAHAM PURSUANT TO 37 CFR § 1.131

Dear Sir:

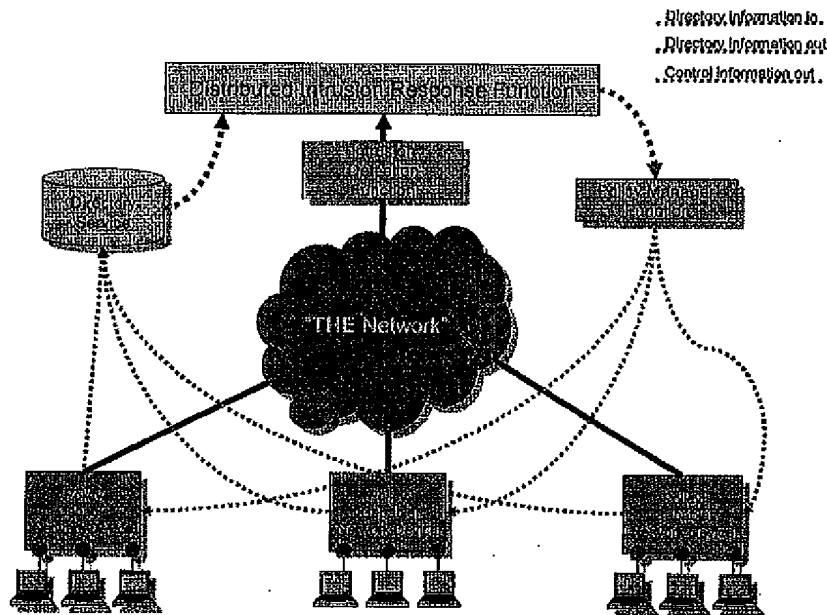
In support of my claim of prior invention of the invention described in the referenced application in view of the Sung et al. reference cited in the January 9, 2008, office action, I hereby declare as follow:

1. My name is Richard Graham. I am an applicant and co-inventor of the invention described and claimed in the referenced patent application.
2. In association with others, I conceived of the invention described in the application before April 14, 2003. On January 2, 2003, I received from co-inventor Richard Bussiere a copy of an email communication sent to Chris Caseiro, the patent attorney processing the referenced application. A copy of the January 2, 2003, email message from Mr. Bussiere to Mr. Caseiro that I received was attached to my October 23, 2007, Declaration as Exhibit A. The email communication that I received included a copy of a standard Enterasys Invention Disclosure Form and a supplemental invention description regarding the Distributed Intrusion Response System described in the referenced patent application. A copy of the standard Enterasys Invention Disclosure Form as I received it on January 2, 2003, was attached to my October 23, 2007, Declaration as Exhibit B. A copy of the supplemental invention description as I received it on January 2, 2003, was attached to my October 23, 2007, Declaration as Exhibit C.
3. I have reviewed Exhibit C of my previously filed declaration and have compared the information contained in that evidence with currently pending independent Claims 1 and 30 of

the present application. I note that elements from those claims are described in Exhibit C as follows:

In Claim 1:

"A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and a plurality of interconnection devices" is represented in the figure on the second page of Exhibit C:



"establishing signal transfer policies for each of a plurality of interconnection devices of the network system" is described on the first page of Exhibit C:

- Policy Capable Network Devices, which are capable of enforcing L2, L3, and L4 policies in any combination

"monitoring the network system for intrusions" is described on the first page of Exhibit C:

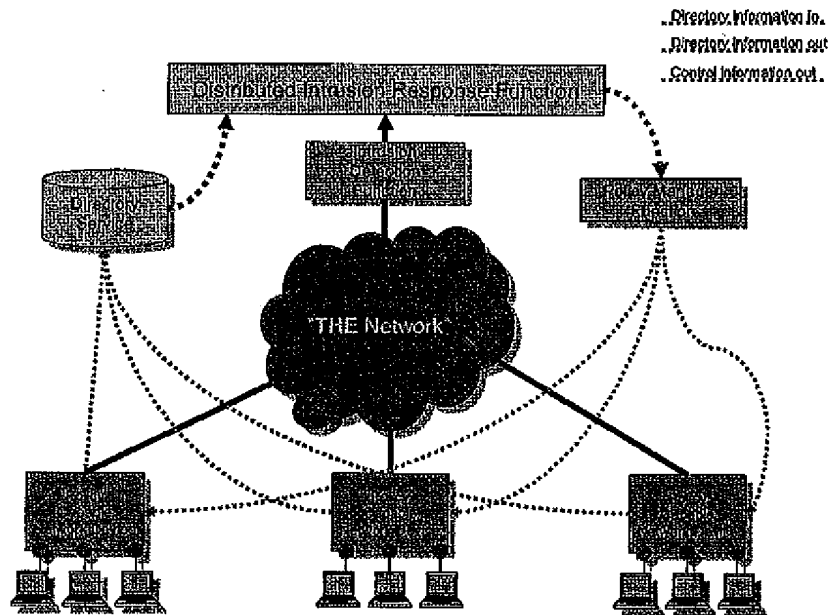
- A centralized or distributed Intrusion Detection Function or systems; which monitor the network or networks for malicious or potentially malicious activities

"upon detection of one or more intrusions of the network, selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions" is described on the third page of Exhibit C:

- Distributed Intrusion Response Function requests that Policy Manager Function modify security policy being applied— Policy Manager applies policy

In Claim 30:

“A network system including a plurality of attached functions, and the network system including the capability to respond to intrusions thereof” is represented in the figure on the second page of Exhibit C:



“an intrusion detection function for identifying one or more sources of one or more intrusions of the network system” is described on the first page of Exhibit C:

- A centralized or distributed Intrusion Detection Function or systems; which monitor the network or networks for malicious or potentially malicious activities

“a plurality of interconnection devices for transferring signals through the network system, wherein each of the plurality of interconnection devices includes one or more signal transfer policies” is described on the first page of Exhibit C:

- Policy Capable Network Devices, which are capable of enforcing L2, L3, and L4 policies in any combination

“a function of a policy enforcement module to change selectively the signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions” is described on the third page of Exhibit C:

- Distributed Intrusion Response Function requests that Policy Manager Function modify security policy being applied— Policy Manager applies policy

4. Upon information and belief, the accompanying Declaration of Chris Caseiro identifies specifically contemporaneous evidence of the element of independent Claim 1 of “excluding from at least one of the plurality of interconnection devices a policy enforcement module for effecting its own signal transfer policy changes” and the element of independent Claim 30 of “wherein at least one of the plurality of interconnection devices excludes the policy enforcement module to establish therein the function to change selectively its own signal transfer policies”.

5. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued.

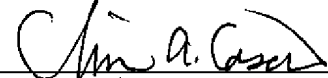
By: 

Richard Graham, Applicant

Date: May 8 2008


Certificate of Transmission

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, using the EFS-Web service of the US Patent Office on May 8, 2008. It is hereby requested that this communication be assigned a receipt date of May 8, 2008.



Chris A. Caseiro